UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/596,038	05/25/2006	Ayako Watanabe	3712174.00609	1948

29175   7590   12/30/2009
K&L Gates LLP
P. O. BOX 1135
CHICAGO, IL 60690

EXAMINER
ZIA, SYED

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
12/30/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

chicago.patents@klgates.com

	Application No.	Applicant(s)
Office Action Summary	10/596,038	WATANABE ET AL.
	Examiner	Art Unit	
	SYED ZIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _15 May 2006_.

2a) ☐ This action is **FINAL**.　　　2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-35_ is/are pending in the application.

　　4a) Of the above claim(s) _14-15,29-30, and 35_ is/are withdrawn from consideration.

5) ☒ Claim(s) _1-13,16-28 and 31-34_ is/are allowed.

6) ☒ Claim(s) _1-13, 16-28, and 31-34_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a) ☒ All　b) ☐ Some * c) ☐ None of:

　　　　1. ☐ Certified copies of the priority documents have been received.

　　　　2. ☐ Certified copies of the priority documents have been received in Application No. _____.

　　　　3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
　　Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
　　Paper No(s)/Mail. Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to application filed May 25, 2006. Claims are 1-35 are

pending.

Response to Arguments

Applicant's arguments filed November 30, 2009 have been considered. Examiner

acknowledges applicant election of Group I Claims (1-13, 16-28, and 31-34) for further

consideration.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed
in the United States before the invention by the applicant for patent or (2) a patent granted on an application for
patent by another filed in the United States before the invention by the applicant for patent, except that an
international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this
subsection of an application filed in the United States only if the international application designated the United
States and was published under Article 21(2) of such treaty in the English language.

Claims 1-13, 16-28, and 31-34 are rejected under 35 U.S.C. 102(e) as being anticipated

by Takashima (U. S. Patent 7,533,224)

The applied reference has a common assignee with the instant application. Based upon

the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C.

102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37

CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the

inventor of this application and is thus not the invention "by another," or by an appropriate

showing under 37 CFR 1.131.

1.   Regarding Claim 1, Takashima teaches and describes an information processing device

comprising: a recording medium interface for executing reading of data from an information

recording medium; and a data processing unit for executing recording processing of new data

either generated or obtained applying information obtained from said information recording

medium; wherein said information recording medium is an information recording medium

storing recorded data in increments of content management units including encrypted data

encrypted by unit keys each of which are set as different encryption keys; and wherein said data

processing unit obtains a unit key corresponding to a content management unit to which said

obtained information belongs or a unit key corresponding to a new content management unit,

executes encryption processing of said new data applying the obtained unit key, and executes

recording processing with the generated encrypted data as data configuring the content

management unit (col.12 line 29 to col.15 line 45, and col.34 line 26 to col. 35 line 49).

2.   Regarding Claim 16, Takashima teaches and describes an information processing method

comprising: a data reading step for reading of data from an information recording medium; and a

data processing step for executing recording processing of new data either generated or obtained

applying information obtained from said information recording medium; wherein said

information recording medium is an information recording medium storing recorded data in

increments of content management units including encrypted data encrypted by unit keys each of

which are set as different encryption keys; and wherein said data processing step includes an

obtaining step for obtaining a unit key corresponding to a content management unit to which said

obtained information belongs or a unit key corresponding to a new content management unit, a

step for executing encryption processing of said new data applying the obtained unit key, and a

step for executing recording processing with the generated encrypted data as data configuring the

content management unit (col.12 line 29 to col.15 line 45, and col.34 line 26 to col. 35 line 49).

3.   Regarding Claim 31, Takashima teaches and describes a computer program for executing

an information processing method, comprising: a data reading step for reading data from an

information recording medium; and a data processing step for executing recording processing of

new data either generated or obtained applying information obtained from said information

recording medium; wherein said information recording medium is an information recording

medium storing recorded data in increments of content management units including encrypted

data encrypted by unit keys each of which are set as different encryption keys; and wherein said

data processing step includes an obtaining step for obtaining a unit key corresponding to a

content management unit to which said obtained information belongs or a unit key corresponding

to a new content management unit, a step for executing encryption processing of said new data

applying the obtained unit key, and a step for executing recording processing with the generated

encrypted data as data configuring the content management unit (col.12 line 29 to col.15 line 45,

and col.34 line 26 to col. 35 line 49).

4.   Claims 2-15, 17-30, and 32-34 are rejected applied as above rejecting Claims 1, 16, and

31. Furthermore, Takashima teaches and describes a system and method identifying multiple digital stream within multiplexed signal, wherein,

As per Claim 2, said data processing unit is configured to set a content management unit corresponding to said new data, and also execute setting processing for an encryption key serving as management information corresponding to the content management unit including said new data (col.13 line 14 tocol.15line 45).

As per Claim 3, said data processing unit is configured to set a content management unit corresponding to said new data, and also execute setting processing for content usage control information serving as management information corresponding to the content management unit including said new data (col.13 line 14 to col.15line 45).

As per Claim 4, said data processing unit is configured to execute writing processing of said new data to a region stipulated by a program included in the information obtained from said information recording medium (col.13 line 14 to col.15line 45).

As per Claim 5, data processing unit is configured to, in a case of storing said new data in storage means other than an information recording medium from which said obtained information has been obtained, execute processing for storing said new data correlated with identification information of the information recording medium from which said obtained information has been obtained (col.13 line 14 tocol.15line 45).

As per Claim 6, said data processing unit is configured to execute encryption processing of an AV stream data file including new data and a navigation file including control information or a program to be applied to playing processing of said AV stream data, and to execute recording processing of new data to storage means (col.28 line 46 to col.31 line 5).

As per Claim 7, said data processing unit is configured to apply a unit key corresponding to a content management unit as an encryption key to be applied to said encryption processing.

As per Claim 8, said data processing unit is configured to execute encryption processing applying, as an encryption key or encryption key generating information, information which can only be obtained by an application licensed to execute processing regarding said content management unit (col.28 line 46 to col.31 line 5).

As per Claim 9, said information which can only obtained by a licensed application is information including a device ID as an identifier unique to the device in which said application is installed (col.28 line 46 to col.31 line 5).

As per Claim 10, said data processing unit is configured to generate a hash value for tampering verification with regard to at least one of an AV stream data file including new data, and a navigation file including control information or a program to be applied to playing processing of said AV stream data, and to record said hash value in storage means (col.28 line 46 to col.34 line 52).

As per Claim 11, said data processing unit is configured to execute data tampering verification processing based on the hash value set for an AV stream data file including new data or a navigation file, at the time of using said file, and executes usage processing of said files under the condition that there is no tampering (col.28 line 46 to col.34 line 52).

As per Claim 12, said data processing unit is configured to execute recording processing of a navigation file, including control information or a program to be applied to playing processing of AV stream data including new data, to storage means, as a file to which an

electronic signature has been appended for tampering verification (col.28 line 46 to col.34 line 52).

As per Claim 13, said data processing unit is configured to execute data tampering verification processing based on the electronic signature set for said AV stream data file including new data or said navigation file, at the time of using said file, and executes usage processing of said files under the condition that there is no tampering (col.28 line 46 to col.34 line 52).

As per Claim 17, said data processing step includes a step for setting of a content management unit corresponding to said new data, and also executing of setting processing for an encryption key serving as management information corresponding to the content management unit including said new data (col.13 line 14 to col.15line 45).

As per Claim 18, said data processing step includes a step for setting of a content management unit corresponding to said new data, and also executing setting processing for content usage control information serving as management information corresponding to the content management unit including said new data (col.13 line 14 to col.15line 45).

As per Claim 19, said data processing step includes a step for executing writing processing of said new data to a region stipulated by a program included in the information obtained from said information recording medium (col.13 line 14 to col.15line 45).

As per Claim 20, in a case of storing said new data in storage means other than an information recording medium from which said obtained information has been obtained, said data processing step executes processing for storing said new data correlated with identification

information of the information recording medium from which said obtained information has been obtained (col.13 line 14 to col.15line 45).

As per Claim 21, further comprising an encryption recording processing step of encryption processing of an AV stream data file including new data and a navigation file including control information or a program to be applied to playing processing of said AV stream data, and executing recording processing of new data to storage means (col.28 line 46 to col.31 line 5).

As per Claim 22, said encryption recording processing step is a step for executing encryption processing, applying a unit key corresponding to a content management unit as an encryption key to be applied to said encryption processing (col.28 line 46 to col.31 line 5).

As per Claim 23, said encryption recording processing step is a step for executing encryption processing, applying, as an encryption key or encryption key generating information, information which can only be obtained by an application licensed to execute processing regarding said content management unit (col.28 line 46 to col.31 line 5).

As per Claim 24, said information which can only be obtained by a licensed application is information including a device ID as an identifier unique to the device in which said application is installed (col.28 line 46 to col.31 line 5).

As per Claim 25, further comprising a step for generating of a hash value for tampering verification with regard to at least one of an AV stream data file including new data, and a navigation file including control information or a program to be applied to playing processing of said AV stream data, and recording of said hash value in storage means (col.28 line 46 to col.34 line 52).

As per Claim 26, further comprising a step for executing data tampering verification processing based on the hash value set for said AV stream data file including new data or said navigation file, at the time of using said file, and executing of usage processing of said files under the condition that there is no tampering (col.28 line 46 to col.34 line 52)

As per Claim 27, further comprising a step for executing recording processing of a navigation file, including control information or a program to be applied to playing processing of AV stream data including new data, to storage means, as a file to which an electronic signature has been appended for tampering verification (col.28 line 46 to col.34 line 52).

As per Claim 28, further comprising a step for executing data tampering verification processing based on the electronic signature set for said AV stream data file including new data or said navigation file, at the time of using said file, and executing of usage processing of said files under the condition that there is no tampering (col.28 line 46 to col.34 line 52).

As per Claim 32, further comprising an encryption recording processing step for executing of encryption processing of an AV stream data file including new data, and a navigation file including control information or a program to be applied to playing processing of AV stream data including new data, and recording to recording means (col.28 line 46 to col.34 line 52).

As per Claim 33, further comprising a step for recording, to storage means, tampering verification data regarding at least one of an AV stream data file including new data, and a navigation file including control information or a program to be applied to playing processing of AV stream data including new data, and recording to recording means (col.28 line 46 to col.34 line 52).

As per Claim 34, further comprising a step for executing data tampering verification processing based on the tampering verification data set for said AV stream data file including new data or said navigation file, at the time of using said file, and executing of usage processing of said files under the condition that there is no tampering (col.28 line 46 to col.34 line 52).

.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
December 15, 2009
/Syed   Zia/
Primary Examiner, Art Unit 2131